Dialog eLink: Order File History

Network secure communication enciphering key data distributing - retrieving first and second terminal keys from storage located remotely of terminals and generating first and second corresponding partial keys

Patent Assignee: I-CO GLOBAL COMMUNICATIONS HOLDINGS LTD; ICO SERVICES LTD

Inventors: JOHNSTON T F

Patent Family (8 patents, 75 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
GB 2313749	A	19971203	GB 199611411	A	19960531	199751	B
EP 810754	A1	19971203	EP 1997303525	A	19970523	199802	E
WO 1997045981	A1	19971204	WO 1997GB1407	A	19970523	199803	E
AU 199729098	A	19980105	AU 199729098	A	19970523	199821	E
GB 2313749	B	19980513	GB 199611411	A	19960531	199821	E
CA 2206247	A	19971130	CA 2206247	A	19970527	199824	E
JP 11510668	W	19990914	JP 1997541825	A	19970523	199948	E
			WO 1997GB1407	A	19970523		
TW 398118	A	20000711	TW 1997107359	A	19970530	200106	E

Priority Application Number (Number Kind Date): GB 199611411 A 19960531

Patent Details

Patent Number	Kind	Language	Pages	Drawings	Filing Notes
GB 2313749	A	EN	85	16	
EP 810754	A1	EN	29		
Regional Designated States,Original	AT BE DE DK ES FI FR GB GR IE IT LU NL PT SE				
WO 1997045981	A1	EN	58		
National Designated States,Original	AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TR TT UA UG US UZ VN				
Regional Designated States,Original	AT BE CH DE DK EA ES FI FR GB GH GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG				
AU 199729098	A	EN			Based on OPI patent WO

					1997045981
GB 2313749	B	EN		0	
CA 2206247	A	EN			
JP 11510668	W	JA	50		PCT Application WO 1997GB1407
					Based on OPI patent WO 1997045981
TW 398118	A	ZH			

Alerting Abstract: GB A

The method involves retrieving first and second terminal keys (Ka,Kb) from storage located remotely of the terminals. First and second corresponding partial keys (Kpa,Kpb) are generated each comprising a masking function of a corresponding one of the terminal keys. The first partial key (Kpa) is dispatched towards the second terminal, and, dispatching the second partial key (Kpb) towards the first terminal.

The method further entails providing a number (RAND), and in which each masking function is a joint function of the number and a corresponding the terminal key. The first and second functions comprise an exclusive-OR.

USE/ADVANTAGE - For secure communication in e.g. cellular terrestrial system such as GSM or fixed link communication systems, or in store-and-forward systems such as email or Internet. Provides mobile communication using end-to-end encryption across whole communication path that provides improved privacy.

International Classification (Main): H04L-009/00

International Patent Classification

IPC	Level	Value	Position	Status	Version
H04B-0007/212	A	I	L	R	20060101
H04L-0009/08	A	I		R	20060101
H04W-0012/00	A	I		R	20090101
H04B-0007/212	C	I	L	R	20060101
H04L-0009/08	C	I		R	20060101
H04W-0012/00	C	I		R	20090101

Original Publication Data by Authority

Australia
Publication Number: AU 199729098 A (Update 199821 E)
Publication Date: 19980105
Assignee: ICO SERVICES LTD (ICOS-N)
Inventor: JOHNSTON T F
Language: EN
Application: AU 199729098 A 19970523 (Local application)
Priority: GB 199611411 A 19960531

Related Publication: WO 1997045981 A (Based on OPI patent)
Original IPC: H04L-9/08(A) H04Q-7/38(B)
Current IPC: H04B-7/212(R,A,I,M,JP,20060101,20051220,A,L) H04B-7/212(R,I,M,JP,20060101,20051220,C,L) H04L-9/08(R,I,M,EP,20060101,20051008,A) H04L-9/08(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)
Current ECLA class: H04L-9/08B H04Q-7/38S H04W-12/02
Current ECLA ICO class: T04W-12:06

Canada
Publication Number: CA 2206247 A (Update 199824 E)
Publication Date: 19971130
Assignee: ICO SERVICES LTD (ICOS-N)
Inventor: JOHNSTON T F
Language: EN
Application: CA 2206247 A 19970527 (Local application)
Priority: GB 199611411 A 19960531
Original IPC: H04L-9/08(A)
Current IPC: H04B-7/212(R,A,I,M,JP,20060101,20051220,A,L) H04B-7/212(R,I,M,JP,20060101,20051220,C,L) H04L-9/08(R,I,M,EP,20060101,20051008,A) H04L-9/08(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)
Current ECLA class: H04L-9/08B H04Q-7/38S H04W-12/02
Current ECLA ICO class: T04W-12:06

European Patent Office
Publication Number: EP 810754 A1 (Update 199802 E)
Publication Date: 19971203
Gesicherte Kommunikation Secure communication Communication securisee
Assignee: ICO Services Ltd., 1 Queen Caroline Street, London W6 9BN, GB (ICOS-N)
Inventor: Johnston, Thomas Francis, 22A Cleveland Square, London, W2 6DG, GB
Agent: Read, Matthew Charles et al, Venner Shipley Co. 20 Little Britain, London EC1A 7DH, GB
Language: EN (29 pages)
Application: EP 1997303525 A 19970523 (Local application)
Priority: GB 199611411 A 19960531
Designated States: (Regional Original) AT BE DE DK ES FI FR GB GR IE IT LU NL PT SE
Original IPC: H04L-9/08(A) H04Q-7/38(B)
Current IPC: H04B-7/212(R,A,I,M,JP,20060101,20051220,A,L) H04B-7/212(R,I,M,JP,20060101,20051220,C,L) H04L-9/08(R,I,M,EP,20060101,20051008,A) H04L-9/08(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)
Current ECLA class: H04L-9/08B H04Q-7/38S H04W-12/02
Current ECLA ICO class: T04W-12:06
Original Abstract: A method of distributing through a communications network enciphering keys for a secure communications session via said network between first and second terminals (2a,2b) corresponding first and second terminal keys (Ka,Kb) comprising: storing said first and second terminal keys (Ka,Kb) remotely to said terminals (2a,2b); providing a number (RAND); generating first and second corresponding partial keys (Kpa,Kpb) each comprising a corresponding function of said number (RAND) and a corresponding one of said terminal keys (Ka,Kb); and dispatching the first partial key (Ka) towards the second terminal (2b), and vice-versa.
Claim: 1. A method of distributing, through a communications network, enciphering key data for secure communication via said network between first and second terminals (2a,2b) each storing corresponding first and

second terminal keys (Ka,Kb) comprising: storing said first and second terminal keys (Ka,Kb) remotely to said terminals (2a,2b); generating first and second corresponding partial keys (Kpa,Kpb) each comprising a corresponding masking function of a corresponding one of said terminal keys (Ka,Kb); and * dispatching the first partial key (Kpa) towards the second terminal (2b), and vice-versa.

Great Britain
Publication Number: GB 2313749 A (Update 199751 B)
Publication Date: 19971203
Assignee: I-CO GLOBAL COMMUNICATIONS HOLDINGS LTD; KY (ICOG-N)
Inventor: JOHNSTON T F
Language: EN (85 pages, 16 drawings)
Application: GB 199611411 A 19960531 (Local application)
Original IPC: H04L-9/08(A)
Current IPC: H04B-7/212(R,A,I,M,JP,20060101,20051220,A,L) H04B-7/212(R,I,M,JP,20060101,20051220,C,L) H04L-9/08(R,I,M,EP,20060101,20051008,A) H04L-9/08(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)
Current ECLA class: H04L-9/08B H04Q-7/38S H04W-12/02
Current ECLA ICO class: T04W-12:06
Claim: The method involves retrieving first and second terminal keys (Ka,Kb) from storage located remotely of the terminals. First and second corresponding partial keys (Kpa,Kpb) are generated each comprising a masking function of a corresponding one of the terminal keys. The first partial key (Kpa) is dispatched towards the second terminal, and, dispatching the second partial key (Kpb) towards the first terminal. The method further entails providing a number (RAND), and in which each masking function is a joint function of the number and a corresponding the terminal key. The first and second functions comprise an exclusive-OR.|GB 2313749 B (Update 199821 E)
Publication Date: 19980513
Assignee: I-CO GLOBAL COMMUNICATIONS HOLDINGS LTD; KY (ICOG-N)
Inventor: JOHNSTON T F
Language: EN (0 drawings)
Application: GB 199611411 A 19960531 (Local application)
Original IPC: H04L-9/08(A)
Current IPC: H04B-7/212(R,A,I,M,JP,20060101,20051220,A,L) H04B-7/212(R,I,M,JP,20060101,20051220,C,L) H04L-9/08(R,I,M,EP,20060101,20051008,A) H04L-9/08(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)
Current ECLA class: H04L-9/08B H04Q-7/38S H04W-12/02
Current ECLA ICO class: T04W-12:06

Japan
Publication Number: JP 11510668 W (Update 199948 E)
Publication Date: 19990914
Assignee: I-CO GLOBAL COMMUNICATIONS HOLDINGS LTD; KY (ICOG-N)
Inventor: JOHNSTON T F
Language: JA (50 pages)
Application: JP 1997541825 A 19970523 (Local application) WO 1997GB1407 A 19970523 (PCT Application)
Priority: GB 199611411 A 19960531
Related Publication: WO 1997045981 A (Based on OPI patent)
Original IPC: H04L-9/08(A) H04B-7/212(B) H04Q-7/38(B)
Current IPC: H04B-7/212(R,A,I,M,JP,20060101,20051220,A,L) H04B-7/212(R,I,M,JP,20060101,20051220,C,L) H04L-9/08(R,I,M,EP,20060101,20051008,A) H04L-

9/08(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)
Current ECLA class: H04L-9/08B H04Q-7/38S H04W-12/02
Current ECLA ICO class: T04W-12:06

Taiwan
Publication Number: TW 398118 A (Update 200106 E)
Publication Date: 20000711
Assignee: ICO SERVICES LTD; GB (ICOS-N)
Language: ZH
Application: TW 1997107359 A 19970530 (Local application)
Priority: GB 199611411 A 19960531
Original IPC: H04L-9/00(A)
Current IPC: H04L-9/00(A)
Current ECLA class: H04L-9/08B H04Q-7/38S H04W-12/02
Current ECLA ICO class: T04W-12:06

WIPO
Publication Number: WO 1997045981 A1 (Update 199803 E)
Publication Date: 19971204
SECURE COMMUNICATION
Assignee: ICO SERVICES LTD., GB (ICOS-N)
Inventor: JOHNSTON, THOMAS, FRANCIS, GB
Language: EN (58 pages)
Application: WO 1997GB1407 A 19970523 (Local application)
Priority: GB 199611411 A 19960531
Designated States: (National Original) AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TR TT UA UG US UZ VN (Regional Original) AT BE CH DE DK EA ES FI FR GB GH GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG
Original IPC: H04L-9/08(A) H04Q-7/38(B)
Current IPC: H04B-7/212(R,A,I,M,JP,20060101,20051220,A,L) H04B-7/212(R,I,M,JP,20060101,20051220,C,L) H04L-9/08(R,I,M,EP,20060101,20051008,A) H04L-9/08(R,I,M,EP,20060101,20051008,C) H04W-12/00(R,I,M,EP,20090101,20090105,A) H04W-12/00(R,I,M,EP,20090101,20090105,C)
Current ECLA class: H04L-9/08B H04Q-7/38S
Original Abstract: A method of distributing through a communications network enciphering keys for a secure communications session via said network between first and second terminals (2a, 2b) corresponding first and second terminal keys (Ka, Kb) comprising: storing said first and second terminal keys (Ka, Kb) remotely to said terminals (2a, 2b); providing a number (RAND); generating first and second corresponding partial keys (Kpa, Kpb) each comprising a corresponding function of said number (RAND) and a corresponding one of said terminal keys (Ka, Kb); and dispatching the first partial key (Kpa) towards the second terminal (2b), and vice versa.

Derwent World Patents Index

Dialog® File Number 351 Accession Number 8434332

Secure communication

Publication number:	JP11510668 (T)
Publication date:	1999-09-14
Inventor(s):	
Applicant(s):	
Classification:	
- international:	***H04B7/212; H04L9/08; H04W12/00;*** **H04B7/212**; **H04L9/08**; **H04W12/00**; (IPC1-7): H04B7/212; H04L9/08; H04Q7/38
- European:	H04L9/08B; H04Q7/38S; H04W12/02
Application number:	JP19970541825T 19970523
Priority number(s):	WO1997GB01407 19970523; GB19960011411 19960531

Also published as:

- EP0810754 (A1)
- TW398118 (B)
- WO9745981 (A1)
- GB2313749 (A)
- CA2206247 (A1)

more >>

Abstract not available for JP 11510668 (T)
Abstract of corresponding document: **EP 0810754 (A1)**

A method of distributing through a communications network enciphering keys for a secure communications session via said network between first and second terminals (2a,2b) corresponding first and second terminal keys (Ka,Kb) comprising: storing said first and second terminal keys (Ka,Kb) remotely to said terminals (2a,2b); providing a number (RAND); generating first and second corresponding partial keys (Kpa,Kpb) each comprising a corresponding function of said number (RAND) and a corresponding one of said terminal keys (Ka,Kb) ; and dispatching the first partial key (Ka) towards the second terminal (2b), and vice-versa.

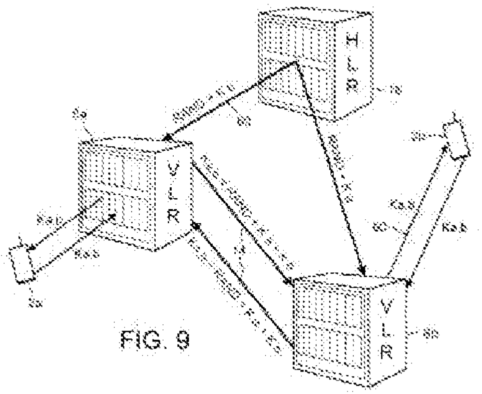

FIG. 9

Data supplied from the ***espacenet*** database — Worldwide